Atari Online News, Etc.
A-ONE Online Magazine
Dana P. Jacobson, Publisher/Managing Editor
Joseph Mirando, Managing Editor
Rob Mahlert, Associate Editor

Atari Online News, Etc. Staff

Dana P. Jacobson -- Editor
Joe Mirando -- "People Are Talking"
Michael Burkley -- "Unabashed Atariophile"
Albert Dayes -- "CC: Classic Chips"
Rob Mahlert -- Web site
Thomas J. Andrews -- "Keeper of the Flame"

With Contributions by:

Fred Horvat

To subscribe to A-ONE, change e-mail addresses, or unsubscribe, log on to our website at: www.atarinews.org and click on "Subscriptions".
OR subscribe to A-ONE by sending a message to: dpj@atarinews.org and your address will be added to the distribution list.
To unsubscribe from A-ONE, send the following: Unsubscribe A-ONE
Please make sure that you include the same address that you used to subscribe from.

To download A-ONE, set your browser bookmarks to one of the following sites:

http://people.delphiforums.com/dpj/a-one.htm
Now available:
http://www.atarinews.org

Visit the Atari Advantage Forum on Delphi!
http://forums.delphiforums.com/atari/

=~=~=~=

A-ONE #1601 01/03/14

~ Facebook Privacy Suit! ~ People Are Talking! ~ Ransomware Evolves!
~ Snapchat Users Hacked! ~ Amazon and Sales Taxes! ~ New, Bigger iPad?
~ FireEye Buys Mediant! ~ Snapchat Offers Opt Out! ~ Reasons Not To Hire!

~ Erase All Your Facebook ~ Coinye West Virtual Coin ~ Leaders on Twitter!

-* NSA: PC To Crack Privacy Codes *-
-* Xbox One Almost Fatally Sabotaged! *-
-* Sony Patent, New Content to Emulated Games *-

=~=~=~=

->From the Editor's Keyboard "Saying it like it is!"
""""""""""""""""""""""""""""

Happy New Year, everyone! The new year is starting out with plenty of new snow and temperature hovering around (and below) zero degrees! I haven't felt this kind of cold for a long time; and the wind makes it feel even colder! Hopefully, your weather is a little bit better.

So, while I find ways to stay warm, and likely you as well, sit back, and enjoy the first issue of the new year!

Until next time...

=~=~=~=

->In This Week's Gaming Section - Microsoft Almost Fatally Sabotaged The Xbox One!
""""""""""""""""""""""""""""""" New Sony Patent, Adding New Content to Emulated Games!

=~=~=~=

->A-ONE's Game Console Industry News - The Latest Gaming News!
""""""""""""""""""""""""""""""""""""

Microsoft Almost Fatally Sabotaged The Xbox One

Microsoft made a lot of terrible public relations mistakes when it rolled out the Xbox One, but thankfully none of those mistakes were reflected in the actual console, which has lived up to the hype and was a hot seller over the holiday shopping season. But in an interview with the Official Xbox Magazine, Microsoft Studios boss Phil Spencer reveals

that Microsoft actually came incredibly close to making a design decision that would likely have handed Sony an easy victory in the latest console wars.

Essentially, Spencer says that Microsoft was still considering removing the Xbox One s disc drive as late as mid-2013 and selling all games digitally over the Internet. While such non-disc-based games probably are the future of console gaming, releasing a console that didn t allow for any disc-based games in 2013 would have been a disastrous mistake because many potential Xbox customers lack the high-speed connections that are needed to make such a system viable. What s more, in an age where ISPs have started slapping subscribers with bandwidth caps, it s very difficult to see how gamers could regularly download enormous files onto their consoles without getting hit with unwelcome overage fees.

There was a real discussion about whether we should have an optical disc drive in Xbox One or if we could get away with a purely disc-less console, but when you start looking at bandwidth and game size, it does create issues, Spencer acknowledge. So we decided which I think was the right decision to go with the Blu-ray drive and give the people an easy way to install a lot of content. From some of those original thoughts, you saw a lot of us really focusing on the digital ecosystem you see on other devices thinking of and building around that.

It goes without saying that happy Xbox One owners are breathing a sigh of relief that Microsoft made this decision.

New Sony Patent Deals With Adding New Content to Emulated Games

A patent filed for by Sony in 2012 has been published today by the United States Patent & Trademark Office, revealing the company’s apparent interest in finding ways to more easily introduce new content into classic games being streamed through the cloud. Essentially, the patent describes the ability to suspend gameplay in an emulated game and then introduce new content in a manner that doesn’t involve reverse engineering the game’s code.

"Finding new ways to play preexisting video games can increase the longevity of older games," the patent states. "Instead of replaying the same level or completing the same missions repeatedly, gamers often desire new challenges when replaying legacy games. In response to this need, game designers have begun to produce mini-games. Within a mini-game, the gamer can be instructed to complete new objectives or challenge their friends for high scores in a format that was not originally designed into the legacy game."

Basic examples of the types of mini-games the patent is referring to are limiting the number of lives or amount of health players have when fighting a boss.

Sony’s patent, which is entitled "Suspending State of Cloud-Based Legacy Applications," would allow for triggers or "snapshots" to be used as the mechanism through which the emulated game is suspended and the new content is then delivered. It also talks about offering games on platforms they were not originally designed for, which is what you’d expect from cloud-based gaming.

Put as simply as possible, "The present disclosure is related to video game emulation. Among other things, this application describes a method and apparatus for emulating a video game that includes generating snapshots that can be used for incorporating new content into the emulated video games."

While it’s unclear what Sony would do if granted the patent, it should be reiterated that this deals with cloud-based game streaming. The patent was originally filed on June 29, 2012, just prior to the company’s announcement of its acquisition of cloud gaming service Gaikai. Sony has announced it will make use of Gaikai on PlayStation 4 - including the ability to stream PS3 games to the system, a feature purportedly coming this year - but it has never given any indication it planned to do more with it than stream games as they already exist.

It’s already been suggested this patent could allow for Sony to release games in the style of NES Remix, which offers twists on levels from classic NES games like Donkey Kong, Excitebike, and Super Mario Bros. Do you have any theories or hopes for what we’ll see from Sony involving this patent, if anything? Let us know in the comments below.

Thanks, NeoGAF.

=~=~=~=

A-ONE’s Headline News
The Latest in Computer Technology News
Compiled by: Dana P. Jacobson

NSA Developing Computer To Crack Privacy Codes

The U.S. National Security Agency is trying to develop a computer that could ultimately break most encryption programs, whether they are used to protect other nations’ spying programs or consumers’ bank accounts, The Washington Post reported on Thursday.

The report, which the newspaper said was based on documents leaked by former NSA contractor Edward Snowden, comes amid continuing controversy over the spy agency’s program to collect the phone records Internet communications of private citizens.

In its report on Thursday, The Washington Post said that the NSA is trying to develop a so-called "quantum computer" that could be used to break encryption codes used to cloak sensitive information.

Such a computer, which would be able to perform several calculations at once instead of in a single stream, could take years to develop, the newspaper said. In addition to being able to break through the cloaks meant to protect private data, such a computer would have implications for such fields as medicine, the newspaper reported.

The research is part of a $79.7 million research program called "Penetrating Hard Targets," the newspaper said. Other, non-governmental

researchers are also trying to develop quantum computers, and it is not clear whether the NSA program lags the private efforts or is ahead of them.

Snowden, living in Russia with temporary asylum, last year leaked documents he collected while working for the NSA. The United States has charged him with espionage, and more charges could follow.

His disclosures have sparked a debate over how much leeway to give the U.S. government in gathering information to protect Americans from terrorism, and have prompted numerous lawsuits.

Last week, a federal judge ruled that the NSA's collection of phone call records is lawful, while another judge earlier in December questioned the program's constitutionality. The issue is now more likely to move before the U.S. Supreme Court.

On Thursday, the editorial board of the New York Times said that the U.S. government should grant Snowden clemency or a plea bargain, given the public value of revelations over the National Security Agency's vast spying programs.

Government Moves To Appeal Surveillance Ruling

The Obama administration moved Friday to ask the secretive U.S. spy court to allow the National Security Agency to continue collecting every American's telephone records every day, in the midst of dueling decisions in two civilian federal courts about whether the surveillance program is constitutional.

U.S. officials were in the process of requesting an order from the Foreign Intelligence Surveillance Court to renew the NSA phone collection program for 90 more days, said Shawn Turner, a spokesman for the Office of the Director of National Intelligence. Such periodic requests are somewhat formulaic but required since the program started in 2006.

The latest request would be the first since two conflicting court decisions about whether the program is lawful and since a presidential advisory panel recommended that the NSA no longer be allowed to collect and store the phone records and search them without obtaining separate court approval for each search.

Also Friday, government lawyers turned to U.S. Court of Appeals for the District of Columbia Circuit to block one federal judge's decision that threatens the NSA phone records program. The opposing lawyer who spearheaded the effort that led to the ruling said he hopes to take the issue directly to the Supreme Court.

The Justice Department filed a one-page notice of appeal asking the appeals court to overturn U.S. District Judge Richard Leon's ruling last month that the program was likely unconstitutional. The government's move had been expected.

Larry Klayman, who filed the class-action suit against President Barack Obama and top administration national security officials, said he intends to petition the federal appeals court next week to send the case directly to the Supreme Court. Klayman said the move was justified because the NSA

case was a matter of great public importance.

"There are exigent circumstances here," Klayman said. "We can’t allow this situation to continue. The NSA’s continuing to spy on everybody."

Judges sitting on the secretive spy court have repeatedly approved the program for 90-day periods. They also have repeatedly upheld the constitutionality of the program a judicial bulwark that held strong until Leon’s surprise decision last month.

Leon said the NSA’s program was "almost Orwellian," a reference to writer George Orwell’s futuristic novel "1984," and that there was little evidence the operation had prevented terrorist attacks. He ruled against the government but agreed to postpone shutting down the program until the government could appeal.

In a separate case involving the same NSA phone records program, a district judge in New York last month upheld the government’s data collection as lawful. The American Civil Liberties Union, which lost that case, said this week it will appeal to a federal appeals court in New York.

Cryptolocker Ransomware Evolves To Spread on Its Own

The notorious Cryptolocker ransomware, which strongly encrypts victims’ hard drives until a ransom is paid, has taken a turn for the worse it’s evolved from a Trojan into a worm.

This means the uncrackable malware can now propagate itself, rather than relying on gullible humans to open infected email attachments or point their browsers at corrupted Web pages.

"This update is considered significant because this routine was unheard of in other CRILOCK variants," wrote security firm Trend Micro in a recent blog posting, using the company’s own name for the malware. "The addition of propagation routines means that the malware can easily spread, unlike other known CRILOCK variants."

The bug seems to have been re-engineered to spread via USB flash drives and PCs in a two-step process, much in the way bubonic plague was spread among humans and fleas.

Greed plays a part as well; the new variant lurks on file-sharing sites, pretending to be an "activator" that verifies pirated copies of Adobe Photoshop and Microsoft Office.

Victims trying to get those paid software products for free will run the "activators," infecting themselves and copying the malware onto any USB drives that are subsequently plugged into their machines. (So far, Cryptolocker infects only Windows PCs.)

There is a silver lining, although it may be temporary. While older versions of Cryptolocker used domain-generation algorithms (DGAs) to constantly move their command-and-control servers from one Web domain name to another, this new variant uses fixed control-server domains, making them easier for anti-virus software to block.

"This could mean that the malware is still in the process of being refined and improved upon," Trend Micro noted. "Thus, we can expect latter variants to have the DGA capability."

Trend Micro has posted a useful FAQ for readers worried about Cryptolocker. Good anti-virus software should also block most variants.

Snapchat Says Millions of User Accounts Compromised

Snapchat, the red-hot private messaging service, said on Thursday that it knew for months about a security loophole that allowed hackers this week to harvest millions of phone numbers and announced changes to its systems.

An anonymous group called Snapchat DB posted the usernames and phone numbers of 4.6 million Snapchat users on New Year’s Eve, days after the startup - headed by 23-year old founder Evan Spiegel - brushed off warnings that its app still contained security loopholes.

The hacker group, which claimed to be based in the United States and Europe, made the entire database available for download but redacted the last two digits of every phone number. Snapchat DB said it was working to raise awareness about Snapchat’s security holes, not out of malicious intent.

In its first public statement since the leak, Snapchat said in a blog post on Thursday that no "snaps" - the contents of messages - were compromised or accessed as part of the hack.

Snapchat was first alerted to the vulnerability in August by a security group called Gibson Security. Snapchat said it made changes to its system to address the weaknesses, but the company also published a blog post downplaying the threat as "theoretical" on December 27.

Snapchat DB carried out the hack and disclosed the phone numbers just four days later.

The hack was a rare black eye for a high-flying appmaker started by Stanford University undergraduates in 2011. Snapchat has soared in popularity over the past year because it allows its users - mostly teens - to send private pictures and messages that self-destruct after 10 seconds at most.

Snapchat’s immense popularity among young users has made it one of the most closely watched social media companies in the world, and Facebook Inc reportedly offered $3 billion last year in a failed acquisition bid.

Snapchat asks new users for their phone number so that their friends can find them on the service. The phone numbers were not attached to any real names.

Calling the hackers’ disclosure an "abuse" of its system, Snapchat said Thursday that it was first told by security experts in August that its "Find Friends" feature may contain a weakness.

The company did not apologize for the leaks but said it would carry out some changes to prevent further unwanted disclosures.

"We will be releasing an updated version of the Snapchat application that will allow Snapchatters to opt out of appearing in Find Friends after they have verified their phone number," the company wrote. "We're also improving rate limiting and other restrictions to address future attempts to abuse our service."

Rate limiting restricts how many times a party can query the Snapchat servers.

In an email to Reuters, the group claiming to be behind the New Years Eve hack called it "promising" that Snapchat was beginning to address its security vulnerabilities.

"Let's hope they aren't trying to downplay the situation once again and avoid the heat, but instead taking reasonable steps to secure sensitive user information," Snapchat DB said. "Actions speak louder than words."

Snapchat To Let Users Opt Out of Built-In Privacy Flaw

Snapchat is now addressing, after a fashion, the clumsy coding in the Find Friends feature that let angry hackers scrape and post private information about 4.6 million Snapchat app users earlier this week.

"We will be releasing an updated version of the Snapchat application that will allow Snapchatters to opt out of appearing in Find Friends after they have verified their phone number," the company said in a blog posting entitled "Find Friends Abuse" yesterday (Jan. 2).

Left unmentioned was a timeline for the release of the updated version. Nor was there an actual fix for the Find Friends feature, similar versions of which are used by Facebook, Twitter and other online services without corresponding problems or any form of "We're sorry."

"What a shame the firm didn't [feel] comfortable expressing an apology to the 4.6 million Snapchat users who have already had their privacy exposed by this incident," observed British security blogger Graham Cluley.

In many ways, this entire debacle could be seen as Snapchat's own fault.

After initial installation of the Snapchat app on an iOS or Android device, the Find Friends feature queries the user's contact list and runs each telephone number against Snapchat's own list of subscriber cellphone numbers.

If there's a match, the Snapchat app displays the username associated with that number and asks the user if he or she wants to add that username to his or her Snapchat contact list. (Users who disable Find Friends will presumably have to add their Snapchat-using friends manually.)

The problem was that Snapchat hadn't built any query-rate limitations that would block rapid-fire queries attempting to "scrape" the user list.

Two Australian researchers calling themselves Gibson Security discovered that fact and, in their own telling, alerted Snapchat to the flaw last August.

Four months later, they hadn’t received a response, and on Christmas Day, they decided to make the flaw public knowledge by posting it on the Internet along with code that would prove it worked.

Gibson Security told ZDNet that the Snapchat flaw could easily have been fixed. But instead of fixing it, Snapchat dismissed Gibson Security’s code and vulnerability exploit as impractical and unlikely.

"Theoretically, if someone were able to upload a huge set of phone numbers, like every number in an area code, or every possible number in the U.S., they could create a database of the results and match usernames to phone numbers that way," Snapchat said in a blog posting last Friday (Dec. 27).

That’s exactly what the unnamed hacker or hackers who leaked the 4.6 million usernames did. Using the code that Gibson Security had provided, he, she or they rapidly generated millions of possible North American telephone numbers and ran each one through Snapchat’s Find Friends feature, capturing the Snapchat usernames associated with any positive result.

The hackers, who called themselves Snapchat DB and claimed to be acting for the benefit of Snapchat users, posted a list of 4.6 million usernames and partly obscured cellphone numbers online on New Year’s Eve. Since most people unwisely use the same usernames for multiple accounts, such information could be leveraged to hijack accounts with other services.

In yesterday’s blog posting, the Snapchat company said it welcomed security suggestions from independent security researchers, even as it called such research "abuse."

"We want to make sure that security experts can get ahold of us when they discover new ways to abuse our service so that we can respond quickly to address those concerns," the posting read. "The best way to let us know about security vulnerabilities is by emailing us: security@snapchat.com."

A few months ago, Snapchat turned down a $3 billion buyout offer from Facebook.

FireEye Buys Firm That Tied Cyberattacks to China

FireEye Inc. said Thursday it has acquired Mandiant Corp., the firm that linked years of cyberattacks against U.S. companies to a secret Chinese military unit.

FireEye said that the purchase of privately held Mandiant would increase its ability to stop attacks in their early stages.

The company valued the deal at nearly $1 billion. FireEye said it would buy 21.5 million shares and options of its stock worth about $884 million at Thursday’s closing price and pay $106.5 million in cash to former Mandiant investors.

FireEye makes computer-security software. It had a successful initial public offering of stock in September, with the shares nearly doubling in price on the first day of trading. The Milpitas, Calif.-based company said its customers include more than 100 of the Fortune 500 corporations.

Virginia-based Mandiant drew attention last February when it issued a detailed report tracing attacks on 141 companies to a hacking unit in Shanghai that experts believe is part of the Chinese Army’s cyber command. The Chinese government denied the firm’s accusations, but the incident helped the company burnish a reputation in cybersecurity.

Mandiant’s clients include more than one-third of the largest 100 corporations, according to FireEye.

Before the deal was announced, shares of FireEye fell $2.48, or 5.7 percent, to close at $41.13, but they were soaring $9.12, or 22.2 percent, to $50.25 in after-hours trading.

FireEye also said that fourth-quarter revenue would be between $55 million and $57 million, higher than the company’s earlier forecast of $52 million to $54 million. Analysts surveyed by FactSet expected $53.4 million. The company is scheduled to report results after the market closes on Feb. 11.

Including the Mandiant acquisition, FireEye expects 2014 revenue to be $400 million to $410 million.

Facebook Sued for Invading Users Privacy

Two Facebook users this week filed a class action complaint against the social network, Ars Technica reports, alleging that the messaging system inside Facebook is not as private as it s advertised to be, and that the company actively mines for data from personal messages and generates likes based on the content exchanged between users. Facebook described its messaging system as unprecedented, when it comes to privacy controls, but the filing alleges that the company is actually accessing data gathered from chats without the user consent.

 Instead to increase user s comfort with the website and, thereby, increase the amount of information they share, the company makes assurances of user control over privacy settings and messaging options, the filing says. In reality, Facebook never intended to provide this level of confidentiality. Instead, Facebook mines any and all transmissions across its network, including those it labels private, in order to gather any and all morsels of information it can about its users.

The filing further explains how Facebook can access the links contained in private messages exchanges and assign likes on the site s respective Facebook page in case it discovers Like buttons on that website. Furthermore, the plaintiffs say that Facebook uses a combination of software and human screening to comb through private messages, in order to use the available data for various purposes including selling it to interested third parties. According to them, while Facebook does explain what user information it receives, it never explains how it scans, mines and manipulates the content of users private messages.

The plaintiffs seek compensation the greater of either $100 for each day of violation, or $10,000 as well as statutory damages of either $50,000 per class member or three times the amount of actual damages.

In addition to the class action suit against Facebook, a petition on Care2 The Petition Site is asking Facebook to stop stalking our unposted

thoughts on the network. The petition was just a few hundred signatures short of its 28,000 goal at the time of this writing, and it comes in response to the recent discovery that Facebook keeps track of everything a user writes while inside the social network, regardless of whether the message or status update is posted or discarded.

The fact that they are doing this is scary and crazy, remember Facebook has been sharing data with the NSA! We have all written posts and then decided against posting them for various reasons. Now we learn Facebook is looking at these posts. If they choose to save them as they claim their policies enable them to, it could mean that every key stroke entered at Facebook could be sent to a government agency, the petition says. On top of all this is the fact that users chose not to post these comments so they should not be seen by anyone. This is a breach of privacy that goes beyond user-beware, as users don t even know their posts are being viewed.

Why You Should Never Hire Anyone Based on Their Facebook Profile

The person you re thinking of hiring has posted a bunch of pictures of themselves drunkenly vomiting on their cat on their Facebook page does this mean they re a bad fit for your company? The answer, according to research flagged by Forbes Kashmir Hill, is maybe not. The new study, conducted by researchers at Florida State University, Old Dominion University, Clemson University, and Accenture, found that there is no correlation between how prospective employers rated someone s Facebook profile and how well that person actually performed at their job.

Even worse, the researchers found that recruiters on average gave lower ratings to people who had traditionally non-White names and/or who were clearly non-White, which means that using Facebook profiles as a criteria for hiring someone may reinforce racial prejudices. Other reasons why prospective hires drew negative marks for their Facebook pages included the use of profanity, references to sexual activity and religious quotations in other words, things that are completely normal to the vast majority of people in the world.

There s a big allure to using Facebook hiring managers say they want to get a sense of the applicant s character, Clemson researcher Philip Roth tells Forbes. It really appears hard for people to stop themselves from doing it if they don t have an HR background. I wouldn t want to use a Facebook assessment until I had evidence it worked for my organization. There needs to be a track record of this working before you use it. I don t think the track record is there yet.

Here s How To Quickly Erase Everything You ve Ever Done on Facebook

Facebook doesn t have a simple way of deleting specific data from one s timeline including old posts, comments and likes that a person would like to have removed from his or her profile, Slate s Jennifer Golbeck has learned. While the social network lets you easily save a copy of all your activity and lets you close your account for that matter it doesn t have a tool that can help with removing only certain past actions that may not be relevant to you and your Facebook friends.

Golbeck said she averaged about 10 activities per day since joining the network in 2005, which meant she had roughly 30,000 past items to manually delete one by one printed, her full Facebook Timeline log would have taken 2,400 pages.

Deleting 30,000 things takes a long time. In the Activity Log, there s a pencil icon next to each item. Clicking that shows a menu of options. Some items can be truly purged; the Delete option is in the menu itself, Golbeck wrote. On average, it took 20 to 30 minutes to purge a month s worth of posts. After about 12 hours of hand-deleting stories, I decided it was time to automate.

The writer found two open-source tools that can run in Chrome or Firefox to automate the Facebook activity removal process, including Facebook Timeline Cleaner and Absterge. However, the results were not on par with expectations. The former would let the user delete only certain past activities, although it runs for a long time in the browser and can crash depending on workload. The second solution is less subtle: it deletes everything. Even so, some of the deleted posts still reappear on Facebook, whether they have been removed manually or by using an automated program.

The real lesson I learned from this exercise is how difficult it is to manage one s online persona. I had it pretty easy: I was willing to delete everything, Golbeck added. For someone who wants to cull their Timeline more selectively, the automated solutions wouldn t work it could take dozens of hours to clean it up.

While Golbeck doesn t see any value in having her entire activity history still available inside Facebook, the social network may certainly be interested in all those posts, status updates and likes to better serve her ads. Last month, it was discovered that Facebook keeps track of everything a customer writes while visiting the social network, even if he or she doesn t end up posting a status or message, in an attempt to better understand user behavior.

Amazon Is Now Charging Sales Tax in Indiana, Nevada, and Tennessee

Three more states have joined the growing list where you'll be charged sales tax on Amazon purchases: Indiana, Nevada, and Tennessee. Amazon already collected tax in 16 states, and in 2016, South Carolina will join them, bringing the number up to an even 20. Technically speaking, you're supposed to add up purchases on your tax returns (the "use tax") no matter where you are, but that oft-ignored rule has increasingly given way to automatic point-of-sale charges. This hasn't happened without strong pushback from Amazon and other online retailers, though; they've gone through several long legal slogs as states pursue sales revenue and parity for local brick-and-mortar businesses.

Amazon's warehouse expansions have given it a physical presence in more and more regions, speeding up deliveries but also opening it up to taxes, but pulling out of a state isn't necessarily a panacea. Recently, the Supreme Court declined to hear an Amazon lawsuit against New York, after the company attempted to fight a ruling that its relationships with local affiliates constituted a physical presence. Though it opposes what it calls a patchwork of state-level taxes, Amazon supports Congressional

efforts to establish nationwide online sales tax rules.

Kanye West-themed Bitcoin Clone Said To Launch This Month

Coders have announced that a new Kanye West-themed cryptocurrency called Coinye West will launch on January 11th. Coinye is based on Bitcoin, the virtual currency that approximates cash on the internet, but will be easier to use, the creators say. "Coinye West is a cryptocurrency for the masses," the creators tell Noisey.

The effort may be nothing more than an elaborate joke, but launching a cryptocurrency is actually relatively easy since the Bitcoin source code is public. Many serious and half-serious clones have launched, but Coinye and the meme-cenric Dogecoin are getting a lot more attention than Litecoin, Namecoin, and other virtual currencies that attempt to improve upon Bitcoin. Perhaps Snoopcoin is next?

Apple s Upcoming 12-inch iPad May Hammer The Notebook Market

Apple and Google have both already done a lot to shake up the traditional PC market but don t expect either of them to stop anytime soon. Barron s flags a note from Evercore Partners analyst Patrick Wang, who thinks that Apple s upcoming 12- to 13-inch iPad has the potential to transform the traditional notebook market as we know it because it will be the first time that Apple has made an iPad that s targeted specifically toward Microsoft s PC customer base.

 Arriving in fall 14, Apple goes Enterprise with an 12-inch iPad, Wang writes. Powered by the A8 chip (perhaps 4C), this expands ARM s reach and, once again, transforms the traditional notebook market as we know it. Expect a 2-1 hybrid think iPad + MBA similar to how most iPads are used in the workplace and in the same spirit of MSFT s Surface.

As Wang acknowledges, Apple isn t really doing something innovative as far as form factor goes since it s basically releasing a new version of the iPad that will be built like Microsoft s Surface. So why would companies flock to the Apple device instead toward devices such as the Surface Pro? One answer could be that the iPad already enjoys a robust app ecosystem that isn t at all lacking for developers. Another is that workers who have iPhones and iPads at home are already familiar with iOS so in theory there shouldn t be the same sort of learning curve that comes with Windows 8.

What s particularly interesting about Apple s upcoming iPad Pro, however, is the specific market that it will reportedly target: Schools. We ve read reports that Google has been making major inroads into schools with its low-cost, low-maintenance Chromebook laptops, so it looks like Microsoft rivals smell blood when comes to displacing PCs as the default computing machines in schools.

Any way you slice it, it looks like Apple and Google are going to keep aggressively invading Microsoft s territory throughout the year.

AllThingsD Editors Launch "Re/code" Venture With NBCUniversal Backing

Veteran technology journalists Walt Mossberg and Kara Swisher have unveiled "Re/code," a technology news site and conference business to succeed AllThingsD which they founded and built into a premier tech media brand within News Corp.

Mossberg and Swisher, who agreed in September to sever a 10-year relationship with News Corp, said on Thursday their new venture will be backed by Comcast's NBCUniversal and Windsor Media, the investment company headed by former Yahoo! Inc Chief Executive Terry Semel.

Mossberg and Swisher will hold majority ownership in the venture, with NBCUniversal and Windsor Media sharing a minority stake.

"It says a lot about NBC in particular that a big media company would take a small share of a startup, provide plenty of funding without trying to control it," Mossberg said by phone. "In order to grow, we needed a fully independent structure."

Mossberg declined to discuss financial details of the deal or the valuation of his new company, but said Re/code will share editorial resources with NBCUniversal.

Re/code's journalists, which include many former AllThingsD staff, will appear on programs such as CNBC and NBC News, while sites such as msnbc.com will run their work. Re/code will also partner with CNBC to host conferences.

Both long-time Wall Street Journal reporters, Swisher and Mossberg founded AllThingsD in 2003 as an annual technology industry gathering.

The blog launched in 2007 and in 2007 News Corp acquired Dow Jones, and with it the profitable AllThingsD. With the dissolution of AllThingsD's relationship with News Corp, the site will remain online but the brand will be phased out.

In the absence of AllThingsD - and with the introduction of a new competitor - the Journal has announced a new technology section complete with gadget reviews (formerly written by Mossberg) and beefed-up coverage from its San Francisco and bureaus in Asia and Israel.

But neither the Journal nor Re/code will inherit the crown jewel of the AllThingsD brand - the lucrative annual conferences that regularly drew names like Steve Jobs, the late Apple Inc chief executive.

The Journal said it would begin hosting its own tech conference called WSJD in late October in southern California.

Mossberg said the same team that produced the AllThingsD conference will produce a rebranded event called the "Code Conference" during the same week and at the same hotel.

Re/code is just one of several new arrivals in the crowded tech media arena.

Earlier this year, Jessica Lessin, another Wall Street Journal reporter, also defected to launch The Information, a premium, subscription-based

tech news site. Yahoo is also preparing a consumer tech site with David Pogue, the former New York Times gadget reviewer.

"Tech sites and tech conferences are areas that people think are in demand and can be both journalistically valuable and financially successful," Mossberg said. "We're obviously hoping the same."

Microsoft CEO Prospects Fear Ballmer Looking Over Their Shoulders

Why is it taking Microsoft so long to find a new CEO? Unnamed sources tell The Wall Street Journal that candidates are worried about the potential influence of Microsoft cofounder Bill Gates and outgoing CEO Steve Ballmer, both of whom are likely to remain on the company s board of directors even after the new CEO is chosen. Specifically, one source says that CEO candidates know that part of what they are negotiating for is the level of engagement that Gates and Ballmer will have with the company after they re hired. The Journal s sources also say that some candidates for the top post at Microsoft seem to be particularly uneasy about Mr. Ballmer, who has made several recent decisions that have altered the company s strategy and generated controversy among managers and investors.

80% of World Leaders Are On Twitter

Twitter isn't just for all those silly youths with their "rap music" and "irony" anymore. According to a recent study, it's also now home to 80% of the world's leaders.

The Digital Policy Council has just released World Leaders on Twitter, the organization's fifth annual report measuring world leaders' activity on the social media site. Their findings determined that a huge majority 80% of world leaders are now tweeting, up 8% from 2012, and up nearly 93% from 2011.

The study also ranked the top ten most popular world leaders on Twitter, with President Obama clocking in in first place (#obvi). In second place is the President of Indonesia, which was really surprising until we learned that 6.5% of all Twitter users come from Indonesia. Who knew!

Here's the full list:

1. President Obama

https://twitter.com/BarackObama/status/415928561485094912

2. President Susilo Bambang Yudhoyono of Indonesia

https://twitter.com/SBYudhoyono/status/419059554039513089

3. President Abdullah Gul of Turkey

https://twitter.com/PresidGul_CIMUN/status/277074875628277761

4. Queen Rania, the Queen Consort of the King of Jordan

https://twitter.com/QueenRania/status/400634374724395008

5. Russian Prime Minister Dmitry Medvedev (lol ok)

https://twitter.com/MedvedevRussiaE/status/379232382580051969

6. President Christina Fernandez De Kirchner of Argentina

https://twitter.com/CFKArgentina/status/384051743874494466

7. His Highness Sheikh Mohammed Bin Al Maktoum, Prime Minister of the UAE and Ruler of Dubai

https://twitter.com/HHShkMohd/status/417621611479441408

8. Mexico s President Enrique Pena Nieto

https://twitter.com/EPN/status/400402202516152320

9. President Juan Manuel Santos of Colombia

https://twitter.com/JuanManSantos/status/411316469281325056

10. Brazilian President Dilma Rouseff

https://twitter.com/dilmabr/status/413722513483788289

=~=~=~=